

フェルマーの定理を巡って（Ⅱ）解答

問題 素数は無限に存在することを、背理法によって証明せよ。

素数が無限にあることの証明法はいくつかありますが、今回は最も有名なユークリッドによる証明を用います。

（証明）

素数が有限個（ n 個）しかないと仮定し、その有限個の素数を、 $p_1, p_2, \dots, p_n$ とする。ある数 p を

$$p = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$$

とすると、 p はどの素数 $p_1, p_2, \dots, p_n$ でも割り切ることができない。つまり、 p は $p_1, p_2, \dots, p_n$ でもない $n+1$ 個目の素数となる。これは仮定に矛盾する。 （証明終わり）

問題 $x^4 + y^4 = z^2$ を満たす自然数は存在しないことを証明せよ。

（証明）

これを満たす自然数の組 (x, y, z) が存在すると仮定する。さらに、最小の z を考えると、 x^2, y^2, z は互いに素である。（※2）また、 $(x^2)^2 + (y^2)^2 = z^2$ と見れば自然数の組 (x^2, y^2, z) は原始ピタゴラス数である。よって、前回の議論より互いに素な自然数 p, q ($p > q$) を用いて、以下で表せる。

$$x^2 = p^2 - q^2 \quad \dots (i)$$

$$y^2 = 2pq \quad \dots (ii)$$

$$z = p^2 + q^2 \quad \dots (iii)$$

(i) より、 $x^2 + q^2 = p^2$ であるから、 (x, q, p) も原始ピタゴラス数となる。したがって、全く同様に自然数 s, t を用いて以下で表せる。

$$x = s^2 - t^2$$

$$q = 2st \quad \dots (iv)$$

$$p = s^2 + t^2 \quad \dots (v)$$

(ii), (iv) より、 $y^2 = 4pst$ となる。 p, s, t は各対で互いに素であるから（※3）、 p, s, t はそれぞれ平方数となり、 $(p, s, t) = (l^2, m^2, n^2)$ とできる。これらを(v)に代入すると、 $l^2 = m^4 + n^4$ となる。これは、元の方程式 $x^4 + y^4 = z^2$ の新しい解 (m, n, l) が存在することになるが、

$$\begin{aligned} z &= p^2 + q^2 \\ &> p^2 \geq p = l^2 \geq l \end{aligned}$$

であるから、 z が最小であることに矛盾する。

（証明終わり）

※2 (x^2, y^2, z) が互いに素でないならば、その最大公約数を g とすると、

$(x^2, y^2, z) = (gX, gY, gZ)$ で表せます。これを与式に代入すると $g^2X^2 + g^2Y^2 = g^2Z^2$ となって、両辺 g^2 で割れば、同じ式で $Z < z$ となる解が見つかります。これは z が最小でないことになります。

※3 (v) の式から、 p, s が互いに素でないとすると t も同じ約数をもつことになります。さらに、(iv) の式を見ると q も同じ約数をもつことになりますので、 p, q が互いに素ではなくなり、もっと言えば (x^2, y^2, z) も互いに素ではなくなってしまいます。